PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 6 - numero 986 di mercoledì 21 aprile 2004

Un worm che parla anche...italiano

Un messaggio in lingua italiana invita l'utente ad aprire il documento allegato: si tratta in realtà di una variante del worm NetSky.

Potrebbe causare una "epidemia" tra gli utenti italiani la nuova variante del worm NetSky individuata nella giornata di ieri.
NetSky.x è "multilingue", una delle tipologie del messaggio di posta elettroniche tramite il quale si diffonde è un messaggio in lingua italiana.
Il soggetto del messaggio italiano è "Re: documento" ed il corpo del messaggio recita. "Legga prego il documento.". L'allegato infetto è invece scelto tra i seguenti: belge.pif, dokumenten.pif, dokumentoida.pif, udokumentowac.pif, dokumentet.pif, original.pif, documento.pif, dokument.pif, document.pif.

Questa variante è molto simile alla precedente infatti condivide circa l'80% del codice e delle caratteristiche di NetSky.U
Nel caso l'allegato sia eseguito, NetSky.X copia se stesso nella cartella Windows e modifica alcune chiavi di registro.
Secondo quanto reso noto da Symbolic, azienda di sicurezza informatica, NetSky.X prima di iniziare a diffondersi via mail raccoglie gli indirizzi da usare per la sua diffusione. Il worm effettua una scansione di tutti i drive da C: a Z: escludendo i CDROM cercando file che hanno varie estensioni, tra le quali .eml, .txt, .php, .cfg, xls, xml.
Una volta trovati i file sono analizzati per cercare eventuali indirizzi email contenuti.
NetSky.X crea diversi tipi di messaggi a seconda del dominio del destinatario; se il domino è .de, ad esempio, il messaggio viene creato in tedesco, se è .it in italiano.
